IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since November 2017. I am currently assigned to the HSI office in Saint Louis, Missouri and am affiliated with the Missouri Internet Crimes Against Children Task Force. I investigate federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I completed training on these and related topics through the Federal Law Enforcement Training Center (FLETC), the National Criminal Justice Training

Center, the National Law Enforcement Training on Child Exploitation, and through various in-service trainings offered through my agency and external partners. That training includes the requirement to observe, review, and classify numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in several forms of electronic media. I am a graduate of the Treasury Computer Forensic Training Program's Basic Computer Evidence Recovery Training and Basic Mobile Device Forensics courses. I hold an A+ certification from the Computing Technology Industry Association. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (production of child pornography), and 2252A(a)(1) & (2) (distribution of child pornography) were committed by Scott Alan BARKER. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and contraband of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

1. On July 5, 2023, I received information from the HSI Cyber Crimes Center (C3) that United Kingdom (UK) law enforcement discovered a video depicting child pornography on the device of a suspect as part of their own ongoing investigation. The video titled "daddy next to son.avi" depicts an adult male sitting in a home with a small male child estimated to be 12 months old on his lap. The adult male exposes his erect penis and masturbates before moving his penis to the child's hand, so they touch, while the adult male continues to masturbate. Believing the video may have originated from the United States, UK law enforcement provided the video to HSI C3 for further investigation.

2. HSI Special Agents assigned to victim identification worked to identify the minor child and the adult suspect depicted in the video, and found a probable match to publicly posted photographs of Scott Alan BARKER of Ashland, MO. Upon receipt of the lead, I personally reviewed the information provided by UK law enforcement, including the video "daddy next to son.avi" and found it meets the definition of child pornography as defined by 18 USC § 2256(8). Further investigation into BARKER, his residence, and publicly available photographs of both led me to apply for a search warrant of BARKER's residence for evidence related to the production of child pornography, which this court issued July 14, 2023 (23-SW-03050-WJE).

3. HSI Special Agents and local law enforcement executed the search on July 17, 2023, and seized 14 items of computer media and took photographs of the interior of the home which matched features seen in the child exploitation video.

4. BARKER provided a post warned statement where he admitted to being the adult male depicted in the child exploitation video, and to using the Omegle online chat website to

communicate with the female persona who UK law enforcement believe was used by the suspect they recovered the child exploitation video from. During the interview, BARKER was asked to list his email addresses. BARKER claimed to have a personal email address that is not used often and is not set up to receive emails on his phone, scottbarker1@outlook.com. BARKER claimed he mainly uses his work email address, sid@amcsportsonline.com. BARKER did not mention or list the SUBJECT ACOCUNTS as used by him.

5. On August 15, 2023, a grand jury in the Western District of Missouri found probable cause to charge BARKER with one count of production of child pornography, 18 USC 2251.

6. Forensic examination of the devices seized from the home is ongoing, but I observed artifacts of the SUJECT ACCOUNTS suggesting use by and attribution to BARKER across multiple devices seized from the residence.

The SUBJECT ACCOUNTS

7. Scottba225@gmail.com – was observed on an ASUS Vivo laptop and an Apple MacBook Pro taken from BARKER's residence both as an autofill value for the Google Chrome application as well as a login to facebook.com. It was also observed on the iPhone 14 Pro with owner name "Scott's iPhone (7)" as a saved user account for the TextNow.com, Facebook, GoPro, and TickPick applications.

8. Scottbarker225@gmail.com – was observed on the ASUS Vivo laptop taken from BARKER's residence as an autofill value for the Google Chrome application. It was also observed on the iPhone 14 Pro with owner name "Scott's iPhone (7)" as a saved Apple ID that was used with iMessage as early as March 2019.

9. Barkerscott225@gmail.com – was observed on the iPhone 14 Pro with owner name "Scott's iPhone (7)" as a saved Apple ID that was used with the iTunes store as early as December 2020.

10. Mgeist543@gmail.com – was observed on the iPhone 14 Pro with owner name "Scott's iPhone (7)" as a saved Apple ID and was used with the iTunes store as early as May 2019 and includes artifacts indicating it is tied to an iCloud account as well as the website hotornot.com.

11. On August 13, 2023, I sent a preservation request to Apple, Inc. to preserve all records pertaining to the SUBJECT ACCOUNTS and Apple responded on August 15, 2023, confirming they preserved all available data for 90 days with reference ID 202300328157.

BACKGROUND CONCERNING APPLE[1]

12. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

13. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

14. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be

linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

15. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

16. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

17. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP

address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

18. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple. Records

and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

19. This investigation involves production and distribution of child pornography which likely may have been committed using a computer device associated with one or more Apple IDs. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

20. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. An iCloud backup of a device may contain historical snapshots of data contained on a device or created by a user even if that device is no longer available or the data has been altered.

21. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant

time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

22. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

23. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

24. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of production or distribution of child pornography including information that can be used to identify the account's user or users, and stored data, including media files, which may reveal further instances of these offenses.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant.

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

27. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

Nicholas Zotos, Special Agent
Homeland Security Investigations

Attested to in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone or other reliable electronic means on tis the 17th day of October 2023.

Willie J. Epps, Jr.
United State Magistrate Judge